

A Channel Coding Approach for Physical-Layer Authentication

Xiaofu Wu* and Zhen Yang*

* Nanjing University of Posts and Telecommunications, Nanjing 210003, CHINA

Emails: xfuwu@ieee.org, yangz@njupt.edu.cn

Abstract—For physical-layer authentication, the authentication tags are often sent concurrently with messages without much bandwidth expansion. In this paper, we present a channel coding approach for physical-layer authentication. The generation of authentication tags can be formulated as an encoding process for an ensemble of codes, where the shared key between Alice and Bob is considered as the input and the message is used to specify a code from the ensemble of codes. Then, we show that the security of physical-layer authentication schemes can be analyzed through decoding and physical-layer authentication schemes can potentially achieve both information-theoretic and computational securities.

Index Terms—Physical-layer authentication, channel coding, decoding complexity, computational security, information-theoretic security.

I. INTRODUCTION

MESSAGE authentication codes (MACs) are cryptographic primitives used extensively in the construction of security services, include authentication, nonrepudiation, and integrity. Basically, message authentication is to ensure that an accepted message truly comes from its acclaimed transmitter. When the transmitter intends to send a message, it also generates a MAC, which is a function of the message and a shared key, known only to both the transmitter and the receiver. The generated MAC is often appended to the message [1]. At the receiver, a MAC is computed from the received message and compared to the MAC that is transmitted. If the two MACs are identical, then the transmitter is identified as a legal user and it is highly likely the received message is exactly equal to the one transmitted.

MAC algorithms can be constructed from other cryptographic primitives, such as cryptographic hash functions or from block cipher algorithms. Currently, the security of MAC algorithms rely on the hardness of hush functions, i.e, given the message and its MAC, it is “hard” to forge a MAC on a new message.

As the development of mobile communications, ensuring security of wireless communications has becoming increasingly important. Openness of wireless networks makes them vulnerable to spoofing attacks where an unauthorized user masquerades as another legitimate user. Although conventional cryptographic security mechanisms can be used to foil such attacks above the physical layer [2], [3]. However, it was believed that more efforts should be done to prevent potential innovative attacks since the wireless medium offers novel avenues for intrusion. In recent years, there has been various

efforts [4]–[7] in authenticating the sender and receiver at the physical layer, based on prior coordination or secret sharing, where the sender is authenticated if the receiver can successfully demodulate and decode the transmission. Among various reported works, it was commonly observed that the physical properties of the wireless medium are a powerful source of domain-specific information that can be used to complement and enhance traditional security mechanisms [4].

In [6], a physical-layer authentication scheme was proposed, in which MACs, along with messages, are transmitted concurrently over the physical layer. Compared to the traditional transmission approach above the physical layer, the authors claims the possibility of information-security due to the introduction of the noise. However, this is not justified in a rigorous way.

In this paper, we provide a channel coding approach for physical-layer authentication. Our contributions include two aspects. Firstly, the computational security can be expressed as the requirement for decoding complexity. Secondly, the information security can be formulated for physical-layer authentication schemes using the standard techniques for a converse proof of channel coding theorem [8].

Throughout this paper, upper case letters (e.g., X) will denote random variables, lower case letters (e.g., x) will denote realizations of the corresponding random variables. and calligraphic letters (e.g., \mathcal{X}) will denote finite alphabet sets over which corresponding variables range. Also, upper case boldface letters (e.g., \mathbf{X}) will denote random vectors whereas lower case boldface letters (e.g., \mathbf{x}) will denote realizations of the corresponding random vectors.

II. A CODING FORMULATION OF PHYSICAL-LAYER AUTHENTICATION

A. Physical-Layer Authentication

Suppose that Alice and Bob agree on a keyed authentication scheme that allows Bob to verify that the messages he receives are from Alice. In order to authenticate, Alice sends an authentication tag (or a MAC), along with a message, for declaring his identity. We call the transmitted signal under this scheme as the tagged signal.

Formally, Alice, as the sender, wants to transmit the authentication tag T together with the message S so Bob (as the receiver) can verify her identity. In general, the tag is a function of the message S and the secret key K

$$T = \tau(S, K), \quad (1)$$

where $\tau : \mathcal{S} \times \mathcal{K} \rightarrow \mathcal{T}$ is a (hash) function.

In order to focus on the essential ideas, we assume here that both the message S and tag T can be denoted as binary random vectors with BPSK modulation. In what follows, we do not discriminate between binary and bipolar vectors, as it can be well understood from the text.

Often, the tag is a short string computed on the message S to be authenticated and the shared secret key K . Let L_s, L_k, L_t denote the length of the message S , the key K and the tag T , respectively. In practice, $L_s \gg L_t$. Here, we always assume that $L_s = QL_t$, where Q is a large integer.

The tag is padded to the message and simultaneously transmitted. The tagged signal (in a discrete column vector form) can be written as

$$\mathbf{u} = \rho_s \mathbf{s} + \rho_t \mathbf{t}_q, \quad (2)$$

where $0 < \rho_s, \rho_t < 1$, $\rho_s^2 + \rho_t^2 = 1$, and $\mathbf{t}_q = \psi(\mathbf{t})$ is a modulation process for modulating a binary tag string \mathbf{t} into the physical discrete-signal vector \mathbf{t}_q , which is chosen to meet $E[\mathbf{s}^H \mathbf{t}_q] = 0$ [6]. Hence, we can interpret ρ_s^2 and ρ_t^2 as energy allocations of the message and tag, respectively.

Essentially, for concurrent transmission of both message and tag, the bit string of a tag should be transmitted with a much lower rate ($\frac{1}{Q}$) than the message symbol rate. In [6], the Haar wavelet is employed for modulating tags. In this paper, we, however, assume a simple repetition function of $\psi(\cdot)$, namely, each component of \mathbf{t} is repeated Q times, which means that

$$\psi(\mathbf{t}) = [\underbrace{t_1, \dots, t_1}_{Q}, \underbrace{t_2, \dots, t_2}_{Q}, \dots, \underbrace{t_{L_k}, \dots, t_{L_k}}_{Q}]^T. \quad (3)$$

This is employed for ease of analysis.

By assuming an additive white Gaussian noise (AWGN) channel model, the received signal vector at Bob can be written as

$$\mathbf{r} = \mathbf{u} + \mathbf{z}, \quad (4)$$

where \mathbf{z} is assumed to an AWGN vector.

As $|\frac{\rho_s}{\rho_t}| \gg 1$ and the signal-to-noise ratio (SNR) is sufficiently high, the transmitted message is assumed to be completely recoverable (often enhanced by error-correcting codes) for both Bob and Eve. Therefore, one can assume that the transmitted signal vector \mathbf{s} is known to both Bob and Eve.

When \mathbf{s} is available at the receiver, it can cancel the message from the received signal samples and the message-free version of a tag can be retrieved [6], which takes the form of

$$\mathbf{y} = \mathbf{x} + \mathbf{w}, \quad (5)$$

where $\mathbf{x} = \mathbf{t}$ and \mathbf{w} is the zero-mean additive white Gaussian noise vector with variance $E[\mathbf{w}_i^\dagger \mathbf{w}_j] = \delta_{ij} \gamma_t^{-1} I_{L_t}$ and γ_t denotes the signal-to-noise ratio (SNR) observed by the authentication tags.

B. A Coding Formulation

Given a message $\mathbf{s} \in \mathcal{S}$, it is possible to generate a code $\mathcal{C}(\mathbf{s})$, which comprised of 2^{L_k} codewords, namely,

$$\mathcal{C}(\mathbf{s}) = \{\mathbf{c}_1(\mathbf{s}), \dots, \mathbf{c}_{2^{L_k}}(\mathbf{s})\}, \quad (6)$$

where each codeword $\mathbf{c}_k(\mathbf{s}) = \tau(\mathbf{s}, \mathbf{k})$ is indexed by a possible key $\mathbf{k} \in \mathcal{K}$ with $k - 1 = \kappa(\mathbf{k})$ denoting the decimal number expression of the binary vector \mathbf{k} . There are $|\mathcal{K}| = 2^{L_k}$ codewords. Now, the code rate of $\mathcal{C}(\mathbf{s})$ can be defined as

$$R_c = \frac{L_k}{L_t}. \quad (7)$$

Consider that Alice wants to authenticate with Bob, she normally sends a message \mathbf{s} , and then a tag $\mathbf{c}_k(\mathbf{s}) = \tau(\mathbf{s}, \mathbf{k})$ is generated using the shared key \mathbf{k} . Equivalently, the generation of the tag for a given message \mathbf{s} can be considered as an encoding process of

$$\tau(\mathbf{s}, \cdot) : \mathcal{K} \rightarrow \mathcal{T}. \quad (8)$$

As the message \mathbf{s} is generated according to a finite message set \mathcal{S} , one have to consider an ensemble of codes $\Omega(\mathcal{C}) = \{\mathcal{C}(\mathbf{s}) : \mathbf{s} \in \mathcal{S}\}$, which is of fixed rate R_c .

This ensemble of codes $\Omega(\mathcal{C})$ is revealed to both Alice and Bob. From a standard cryptographic view, this code ensemble is also revealed to Eve.

Definition 1: The minimum Hamming distance of the code ensemble $\Omega(\mathcal{C})$ can be defined as

$$d_{\min}(\Omega(\mathcal{C})) = \min_{\mathbf{s} \in \mathcal{S}} \min_{\mathbf{k} \neq \hat{\mathbf{k}}} d_H(\tau(\mathbf{s}, \mathbf{k}), \tau(\mathbf{s}, \hat{\mathbf{k}})), \quad (9)$$

where $d_H(\mathbf{c}_1, \mathbf{c}_2)$ denotes the Hamming distance of two binary vectors \mathbf{c}_1 and \mathbf{c}_2 .

Now, the task of physical-layer authentication can be formally formulated as a hypothesis testing problem as follows.

- ♣ Bob decides if \mathbf{y} is from Alice or not by assuming that $\mathbf{s}, \mathbf{k}, \tau(\cdot, \cdot)$ are available;
- ♠ Eve tries to retrieve \mathbf{k} from \mathbf{y} by assuming that $\mathbf{s}, \tau(\cdot, \cdot)$ are available.

III. HYPOTHESIS TESTING

A. General Formulation

To complete the authentication process, Bob requires to verify that whether the response signal \mathbf{y} is from Alice or not. If the response signal is not from Alice but Eve (an impersonation attacker), it is assumed that Eve generates length- L_k binary random vector \mathbf{k}_E for authentication as there is no any information about $\mathbf{k}_A (= \mathbf{k}_B)$ available. Essentially, this is cast as a binary hypothesis testing problem:

$$H_0 : K = \mathbf{k}_B \quad (10)$$

$$H_1 : K = \mathbf{k}_E \quad (11)$$

where K denotes the acknowledged key.

Hypothesis testing is the task of deciding which of two hypotheses, H_1 or H_0 , is true, when one is given the value u of a random variable U (e.g., the outcome of a measurement), namely, $U = u$. In our case, $U = (Y, K)$, $u = (\mathbf{y}, \mathbf{k}_B)$. We begin with the formulation of the optimum binary hypothesis testing, i.e.,

$$\eta = \log \frac{p_{H_0}(U = u)}{p_{H_1}(U = u)} = \log \frac{p(\mathbf{y}, K = \mathbf{k}_B)}{p(\mathbf{y})p(K = \mathbf{k}_B)} \quad (12)$$

$$= \log \frac{p(\mathbf{y}|K = \mathbf{k}_B)}{\sum_{\mathbf{k} \in \mathcal{F}_2^{L_k}} p(\mathbf{y}|K = \mathbf{k})p(K = \mathbf{k})}. \quad (13)$$

We point out that in the case of H_1 , the generation of the message and key is independent to each other as there is no means to efficiently guess the key.

As the message \mathbf{s} is assumed to be available, it is clear that

$$p(\mathbf{y}|\mathbf{k}) \propto \exp \left[-\frac{(\mathbf{y} - \mathbf{t})^\dagger (\mathbf{y} - \mathbf{t})}{2\sigma_w^2} \right] \quad (14)$$

with $\mathbf{t} = \tau(\mathbf{s}, \mathbf{k})$.

In general, this binary hypothesis testing problem in its optimum form can not be easily tackled as it requires to enumerate 2^K binary vectors of \mathbf{k} with a priori uniform distribution. However, its performance can be information-theoretically bounded [9], which is summarized as follows.

B. Detection Probability vs. False Alarm Probability

Let $P_D = 1 - \alpha$ be the detection probability, namely, the probability of successful declaration of H_0 when H_0 is actually true, and $P_f = \beta$ be the false alarm probability, namely, the probability of false declaration of H_0 when H_1 is actually true.

Let the function $d(\alpha, \beta)$ be defined by

$$d(\alpha, \beta) = \alpha \log \frac{\alpha}{1 - \beta} + (1 - \alpha) \log \frac{1 - \alpha}{\beta}. \quad (15)$$

With optimal hypothesis testing (12), its detection probability and false alarm probability are closely connected.

Lemma 1: [9] The detection probability $1 - \alpha$ and the false alarm probability β satisfy

$$d(\alpha, \beta) \leq D_{KL}(p(\mathbf{y}, \mathbf{k}_B) || p(\mathbf{y})p(\mathbf{k}_B)) = I(Y; K) \quad (16)$$

where $I(Y; K)$ denotes the mutual information between two random variables Y and K , and

$$D_{KL}(f(x) || g(x)) = \sum_x f(x) \log \frac{f(x)}{g(x)} \quad (17)$$

for two probability distributions $f(x), g(x)$.

C. A Suboptimal Solution

As the optimum hypothesis testing is difficult to implement, we propose to use a simple test statistic

$$\eta = \mathbf{c}_B^T \mathbf{y}, \quad (18)$$

and ζ is further compared to a threshold value ϱ for making a final decision, where $\mathbf{c}_B = \tau(\mathbf{s}, \mathbf{k}_B)$ is the codeword due to the input of \mathbf{k}_B at Bob.

This approach can be viewed as a code acquisition approach encountered in code-division multiple-access (CDMA) communication systems, where \mathbf{c}_B can be considered as a unique PN code, which is available at the sides of both Alice and Bob, but keeps unknown to any potential attacker.

In both hypotheses, η is the sum of L_t normally distributed random variables, which is still normally distributed. Therefore, it suffices to compute its mean and variance.

In the case of hypothesis H_0 , one can show that

$$\eta|H_0 = L_t + z_0, \quad (19)$$

where $z_0 = \sum_{i=1}^{L_t} c_i^B w_i$. We denote its mean and variance as

$$\begin{aligned} \bar{\eta}_0 &\triangleq E\{\eta|H_0\} = L_t, \\ \sigma_{H_0}^2 &\triangleq \text{Var}\{\eta|H_0\} = L_t \gamma_t^{-1}. \end{aligned} \quad (20)$$

By decomposing the hypothesis H_1 into a series of sub-hypotheses $\{H_1^{sk} : H_1, S = \mathbf{s}, K = \mathbf{k}_E\}$, i.e., by further assuming that the transmitted signal is \mathbf{s} and Eve impersonates Alice using the key \mathbf{k}_E , we have

$$\eta|H_1^{sk} = L_t - 2d_H(\tau(\mathbf{s}, \mathbf{k}_B), \tau(\mathbf{s}, \mathbf{k}_E)) + z_1, \quad (21)$$

where $z_1 = \sum_{i=1}^{L_t} c_i^B w_i$. Then,

$$\begin{aligned} \bar{\eta}_1^{sk} &\triangleq E\{\eta|H_1, \mathbf{s}, \mathbf{k}_E\} = L_t - 2d_H(\tau(\mathbf{s}, \mathbf{k}_B), \tau(\mathbf{s}, \mathbf{k}_E)), \\ \sigma_{H_1^{sk}}^2 &\triangleq \text{Var}\{\eta|H_1, \mathbf{s}, \mathbf{k}_E\} = L_t \gamma_t^{-1}. \end{aligned} \quad (22)$$

It is clear that $\eta|H_0 \sim \mathcal{N}(\bar{\eta}_0, \sigma_{H_0}^2)$ and $\eta|H_1^{sk} \sim \mathcal{N}(\bar{\eta}_1^{sk}, \sigma_{H_1^{sk}}^2)$.

The authentication is typically claimed if $\eta \geq \varrho$. The threshold ϱ of this test is determined for a false alarm probability β according to the distribution of $\eta|H_1$

$$\varrho = \arg \min_{\varrho'} E_{\mathbf{s}, \mathbf{k}_E} \left[Q \left(\frac{\varrho' - \bar{\eta}_1^{sk}}{\sigma_{H_1^{sk}}} \right) \right] \geq \beta, \quad (23)$$

where

$$Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty \exp \left(-\frac{t^2}{2} \right) dt. \quad (24)$$

The detection probability can be simply computed as

$$P_D = Q \left(\frac{\varrho - \bar{\eta}_0}{\sigma_{H_0}} \right). \quad (25)$$

IV. A DECODING APPROACH FOR SECURITY ANALYSIS

For a physical-layer authentication system, we can characterize it using a quadruple $\{\mathcal{S}, \mathcal{K}, \Omega(\mathcal{C}), p(\mathbf{y}|\mathbf{x})\}$. In this paper, we always assume a memory-less channel and hence, $p(\mathbf{y}|\mathbf{x}) = \prod_{i=1}^{L_t} p(y_i|x_i)$.

A. Adversary Model

Eve, as the adversary, is an aware receiver and knows the authentication scheme that Alice and Bob are using. However, she does not know the shared secret key between Alice and Bob. She can be a passive attacker or active attacker. As an active attacker, Eve can perform impersonation attacks.

B. Passive Attacks: A Decoding Approach for Recovery of Key

As a passive attacker, Eve only monitors all frames inside the network during authentication, and tries to learn \mathbf{k}_B from whatever it gets.

Firstly, we consider the noiseless setting as in a classic authentication application above the physical layer, in which Eve can directly acquire the signal \mathbf{s} and the tag $\mathbf{y} = \tau(\mathbf{s}, \mathbf{k}_B)$.

Given \mathbf{s} and if the encoding rule

$$\tau(\mathbf{s}, \cdot) : \mathcal{K} \rightarrow \mathcal{T}$$

is a bijection, Eve can recover the key \mathbf{k} by generating a lookup table of size 2^{L_k} and searching over this table for finding the key \mathbf{k}_E , which admits $\mathbf{y} = \tau(\mathbf{s}, \mathbf{k}_E)$.

In the language of coding, it means that the recovery of key can be considered as decoding of the received signal Y to its maximum possible encoding input $\hat{K}(Y)$. Given s , if any decoder $\hat{K}(Y)$ is of computational complexity $\mathcal{O}(2^{L_k})$, we claim that the computational security can be achieved for this authentication system.

Definition 2: (Computational security) Given a physical-layer authentication system $\{\mathcal{S}, \mathcal{K}, \Omega(\mathcal{C}), p(\mathbf{y}|\mathbf{x})\}$, we claim that this system is computationally secure if for any decoder $\hat{K}(Y)$, its computation complexity is of $\mathcal{O}(2^{L_k})$.

For ensuring computational security, it requires that no any efficient decoding algorithm exists for any code $\mathcal{C}(s) \in \Omega(\mathcal{C})$. Since the publication of Shannon's original paper in 1948, the search of the codes for achieving the channel capacity has come a long way. Currently, linear codes and their efficient decoding algorithms have been extensively studied. Therefore, for construction of a good physical layer authentication system, linear code ensembles should be better avoided as their complexity can often be reduced due to the linearity of codes.

In the classic authentication scenarios, Eve can observe several pairs of (message, tag), namely, $(s_i, t_i = \tau(s_i, \mathbf{k}))$, $i = 1, \dots, I$. For computational security, it means that Eve is still hopeless for getting an estimate of \mathbf{k} with many observation pairs (s_i, t_i) . In the language of coding, this can be well justified as each pair (s_i, t_i) reflects an codeword of $\mathcal{C}(s_i)$. If $s_i \neq s_j$, t_i and t_j reveal the structure of two different codes, i.e., $\mathcal{C}(s_i)$ and $\mathcal{C}(s_j)$.

Secondly, we consider the noise setting, as seen in the physical-layer authentication scenarios.

Definition 3: Let the binary codeword $\mathbf{c} \in C$, which is further modulated with $\mathbf{x}(\mathbf{c})$ and transmitted over the channel $p(\mathbf{y}|\mathbf{x})$, the received vector $\mathbf{y} \in \mathcal{R}^{L_t}$. A maximum-likelihood (ML) decoding algorithm decodes the vector \mathbf{y} into a codeword $\hat{\mathbf{c}}$, such that

$$\hat{\mathbf{c}} = \max_{\mathbf{c} \in C} p(\mathbf{y}|\mathbf{x}(\mathbf{c})). \quad (26)$$

Definition 4: (ML recoverable) Given $\mathbf{y} \in \mathcal{R}^{L_t}$ and s , where $\mathbf{y} = \tau(s, \mathbf{k}) + \mathbf{w}$. For an ML decoder $\hat{\mathbf{k}}(\mathbf{y})$, we mean that

$$\hat{\mathbf{k}} = \max_{\mathbf{k} \in \mathcal{K}} p(\mathbf{y}|\mathbf{k}, s). \quad (27)$$

If $\Pr(\hat{\mathbf{k}} \neq \mathbf{k}_A) = 0$, we claim that the authentication key is ML recoverable.

In what follows, we consider a binary-input continuous-output AWGN channel (Bi-AWGN). Its capacity $C_2(\gamma_t)$ is a function of the signal-to-noise ratio γ_t , which can be explicitly expressed as

$$C_2(\gamma_t) = \left[1 - \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} e^{-(y-\beta)^2/2} \log_2(1 + e^{-2\beta y}) dy \right],$$

where $\beta = \sqrt{2\gamma_t}$.

The SP59 bound of Shannon [10] provides a lower bound on the decoding error probability of block codes transmitted over the AWGN channel. With a coding approach for physical-layer

authentication, the best possible decoding probability with ML decoding for a potential eavesdropper can now be lower bounded with the Shannon's 1959 sphere-packing bound.

Lemma 2: (The 1959 Sphere-Packing Lower Bound [10]) For a physical-layer authentication system, characterized by the quadruple $\{\mathcal{S}, \mathcal{K}, \Omega(\mathcal{C}), p(\mathbf{y}|\mathbf{x})\}$. Let a message $s \in \mathcal{S}$ be sent, and the authentication tags are assumed to be transmitted over a Bi-AWGN channel with the signal-to-noise ratio of γ_t . For any decoder \hat{K} , it is clear that $K \rightarrow \tau(s, K) \rightarrow X \rightarrow Y \rightarrow \hat{K}$ form a Markov process. Let $P_e = \Pr(K \neq \hat{K})$, we have that

$$P_e > P_{SPB}(L_t, \theta, \gamma_t),$$

where

$$P_{SPB}(L_t, \theta, \gamma_t) = Q(\sqrt{2L_t\gamma_t}) + \frac{L_t - 1}{\sqrt{2\pi}} e^{-L_t\gamma_t} \cdot \int_{\theta}^{\pi/2} \sin(\phi)^{L_t-2} f_{L_t}(\sqrt{2L_t\gamma_t} \cos(\phi)) d\phi,$$

$$f_L(x) = \frac{1}{2^{\frac{L-1}{2}} \Gamma(\frac{L+1}{2})} \int_0^{\infty} z^{L-1} \exp\left(-\frac{z^2}{2} + zx\right) dz,$$

and $\theta \in [0, \pi]$ satisfies the inequality $2^{-L_t R} \leq \frac{\Omega_{L_t}(\theta)}{\Omega_{L_t}(\pi)}$ with

$$\Omega_{L_t}(\theta) = \frac{2\pi^{\frac{L_t-1}{2}}}{\Gamma(\frac{L_t-1}{2})} \int_0^{\theta} (\sin(\phi))^{L_t-2} d\phi.$$

The SP59 bound is exponentially increased with the block length and the exponent is strictly negative for all $R_c > C_2(\gamma_t)$, it become clear that above capacity the minimum probability of error goes to 1 exponentially fast with the block length. Hence, one can achieve the information security for physical-layer authentication, which, however, not the case for classic authentication.

Lemma 3: (Information security) Given a physical-layer authentication system $\{\mathcal{S}, \mathcal{K}, \Omega(\mathcal{C})\}$ over an AWGN channel of the SNR γ_t , we claim that this system can achieve information security if $R_c > C(\gamma_t)$ when $L_t \rightarrow \infty$.

Numerically, we'll show that the decoding error probability can go to 1 even with short block length if the signal-to-noise ratio γ_t is sufficiently low.

C. Impersonation Attacks

In a so-called impersonation attack at time i , the adversary (Eve) waits until he has seen the ciphertexts $\{(s_1, t_1), (s_2, t_2), \dots, (s_{i-1}, t_{i-1})\}$ (which he lets pass unchanged to the receiver) and then creates and sends a fraudulent ciphertext (s_i, t_i) which he hopes to be accepted by the receiver as the i th ciphertext.

Essentially, Eve's strategy is to maximize the false acceptance rate by selecting a suitable message s_i and a key \mathbf{k}_E , namely,

$$\max_{s_i \in \mathcal{S}, \mathbf{k}_E \in \mathcal{K}} E\{\eta | H_1, s_i, \mathbf{k}_E\}. \quad (28)$$

Equivalently, this means

$$\min_{\mathbf{s}_i \in \mathcal{S}, \mathbf{k}_E \in \mathcal{K}} d_H(\tau(\mathbf{s}_i, \mathbf{k}_B), \tau(\mathbf{s}_i, \mathbf{k}_E)), \quad (29)$$

as shown by (21).

Lemma 4: In order to minimize the false acceptance rate of an impersonate attacker, the minimum Hamming distance of the code ensemble $\Omega(\mathcal{C})$, namely, $d_{\min}(\Omega(\mathcal{C}))$, should be maximized.

V. NUMERICAL EXAMPLE

Consider a physical-layer authentication system, in which binary key is of length $L_k = 128$ and the authentication tag is of length $L_t = 256$. To attack this physical-layer authentication system, a potential eavesdropper tries to do her or his best to decode the key. As one can consider the block codes of rate R_c over a Bi-AWGN channel of the SNR γ_t , the equivalent E_b/N_0 can be defined as $E_b/N_0 = R_c^{-1}\gamma_t$.

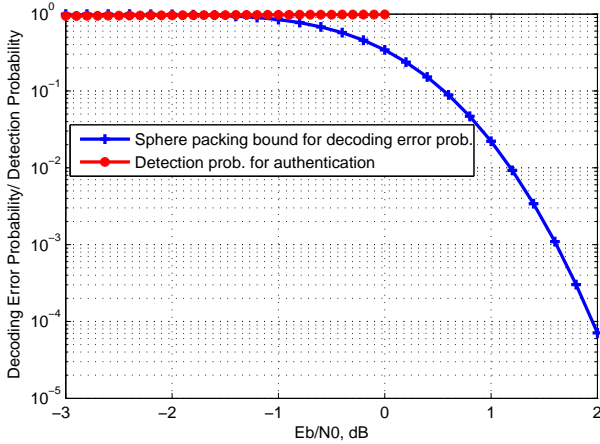


Fig. 1. Sphere-packing low bound on the decoding error probability and detection probability (or successful authentication rate) versus E_b/N_0 .

Fig. 1 shows the SP59 bound on the decoding error probability and detection probability (successful authentication rate) for different E_b/N_0 's. As the eavesdropper cannot do better than a ML decoder, the SPB bound provides an over-estimate of its capability on guessing the key. As shown, the eavesdropper becomes hopeless in guessing the key whenever E_b/N_0 is below to about -1 dB as the decoding error probability is around 1. However, the authentication system does work well with almost perfect successful authentication rate. In simulations, the threshold is set so as the false alarm probability is lower than 0.01.

VI. CONCLUSION

We propose a channel coding approach for physical layer authentication. With this new approach, the computational security for classic authentication schemes can be well formulated using a new decoding approach. The well-designed physical-layer authentication can ensure a new degree of security, namely, information-security, thanks to the introduction of channel noises during transmission.

For design of a physical layer authentication system, the success authentication rate should be balanced with an acceptable false acceptance rate. It is beneficial for use of long tags, as the success authentication rate can be enhanced while the false acceptance rate can be reduced. In the meantime, numerical results show that even with short tags (of length 256), the best possible decoding error probability under ML decoding can approach 1 while the authentication still work well.

ACKNOWLEDGMENT

This work was supported in part by the National Natural Science Foundation of China under Grants 61372123, 61271335, 61032004, 61302103. The work of Wu was also supported by the Scientific Research Foundation of Nanjing University of Posts and Telecommunications under Grant NY213002. The work of Yang was also supported by the Key University Science Research Project of Jiangsu Province under Grant 14KJA510003.

REFERENCES

- [1] B. Schneier, *Applied Cryptography*. New York: Wiley, 1996.
- [2] A. Mishra, M. Shin, and W. A. Arbaugh, "Your 802.11 network has no clothes," *IEEE Commun. Mag.*, vol. 9, pp. 44–51, Dec. 2002.
- [3] M. Shin, J. Ma, A. Mishra, and W. Arbaugh, "Wireless network security and interworking," *Proc. IEEE*, vol. 94, pp. 455–466, Feb. 2006.
- [4] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Using the physical layer for wireless authentication in time-variant channels," *IEEE Trans. Wireless Commun.*, vol. 7, pp. 2571–2579, Jul. 2008.
- [5] D. Shan, K. Zeng, W. Xiang, P. Richardson, and Y. Dong, "PHY-CRAM: Physical layer challenge-response authentication mechanism for wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 31, pp. 1817–1827, 2013.
- [6] P. L. Yu, J. S. Baras, and B. M. Sadler, "Physical-layer authentication," *IEEE Trans. Inf. Forensics Security*, vol. 3, pp. 38–51, Mar. 2008.
- [7] J. K. Tugnait, "Wireless user authentication via comparison of power spectral densities," *IEEE J. Sel. Areas Commun.*, vol. 31, pp. 1791–1802, 2013.
- [8] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. New York: Wiley, 1991.
- [9] U. M. Maurer, "Authentication theory and hypothesis testing," *IEEE Trans. Inf. Theory*, vol. 46, pp. 1350–1356, Jul. 2000.
- [10] C. E. Shannon, "Probability of error for optimal codes in a gaussian channel," *Bell System Technical Journal*, vol. 38, pp. 611–656, May 1959.